STATE of ARIZONA

Government **I**nformation **T**echnology **A**gency	**Statewide** **STANDARD** **P800-S830 Rev 1.0**	**TITLE: Network Security** **Effective Date: April 5, 2004**

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) (A.R.S. § 41-3504(A (1))) including the adoption of statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a)))).

2. PURPOSE

The purpose of this standard is to coordinate budget unit and State efforts to provide a multi-layer protection strategy for secure and seamless interconnections of the State's heterogeneous systems and communications networks, including modems, routers, switches, and firewalls while protecting the State's computing resources and information from the risk of unauthorized access from external sources.

3. SCOPE

This applies to all budget units. Budget unit is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches. A.R.S. § 41-3501(2).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSPs) within each budget unit.

4. STANDARD

The following network security standards provide the minimum requirements for providing secure and seamless interconnection of communications networks and systems while protecting the State's computing resources and information. Multi-layered protection shall be deployed at the Internet gateway, the network server, and the desktop levels to prevent introduction of malicious code or unauthorized access into the State's information systems.

4.1. NETWORK PERIMETER SECURITY**:** Firewall technology shall be employed at the edge of a budget unit's network including the Internet Gateway, to protect sensitive internal information assets and infrastructure from unauthorized access. External (inbound and outbound) traffic shall be routed through secure gateways, such as firewalls.

4.1.1. Network traffic filtering rules for traffic that traverses the Internet shall include the following:

- An incoming packet shall not have a source address of the internal network,
- An incoming packet shall not contain Internet Control Message Protocol (ICMP) traffic,
- An incoming packet shall have a publicly registered destination address associated with the internal network if using static or dynamic Network Address Translation (NAT),
- An incoming packet should not contain Simple Network Management Protocol (SNMP) traffic,
- An outgoing packet shall have a source address of the internal network,
- An outgoing packet shall not have a destination address of the internal network,
- An incoming or outgoing packet shall not have a source or destination address that is private or listed in RFC 1918-reserved space,
- Sources of traffic from Internet sites that are known to contain spam, offensive material, etc., may be blocked at the discretion of the budget unit.

4.1.2 Any source routed packets or any packets with the IP options field set shall be blocked.

4.1.3 Inbound or outbound traffic containing source or destination addresses of 127.0.0.1 or 0.0.0.0, or directed broadcast addresses should be blocked.

4.1.4 Firewall technologies shall have security logging turned on. Logs should be reviewed, on a frequency determined and documented by the budget unit, by budget unit authorized personnel and all incidents, violations, etc. reported and resolved.

4.1.5 Firewall policies should be reviewed, tested, and audited, on a frequency determined and documented by the budget unit.

4.1.6 Remote management of firewall technologies should be via encrypted communications.

4.1.7 Unneeded services shall be turned off and unused ports disabled.

4.1.8 When required to allow converged services, such as voice (VoIP), instant messaging, presence, mobility services, multimedia (MoIP), etc., to securely traverse network borders and NAT functionality, firewall technologies shall:

- Use a SIP proxy server or H.323 gatekeeper outside the firewall, with the firewall configured to allow communication of endpoints only with the proxy server, or
- Be configured to function as application-layer gateways that monitor all SIP and H.323 traffic in order to open and close

restricted ports as required and rewrite the IP addresses within the unencrypted application-layer messages, or

- Use a Session Border Controller, also known as an application router, to allow for end-to-end VoIP communications across multiple IP networks while allowing VoIP endpoints such as VoIP gateways, IP phones, and IP soft phones; which are behind a Network Address Translation (NAT) firewall, to communicate with VoIP endpoints on external IP networks.
- IETF Internet Draft proposals for NAT traversal, such as Connection Oriented Media Transport, Middlebox Communications (Midcom), Simple Traversal of UDP Through NAT (STUN), and Traversal Using Relay NAT (TURN) taken singularly do not provide a complete, universal solution that is applicable to all existing scenarios. IETF Internet Draft Interactive Connectivity Establishment (ICE) is a proposed methodology for NAT traversal for SIP. ICE makes use of existing protocols, such as STUN, TURN, and even Realm Specific IP (RSIP). ICE works through the cooperation of both endpoints in a session.

4.1.9 Budget units may collectively establish inter-agency service agreements (ISAs) to implement and maintain a “trusted peer” relationship among multiple participants. Each participant in the agreement shall agree to conform to all applicable requirements set forth in the agreement to ensure sufficient and acceptable security protection for all other participating entities.

4.2. <u>END POINT SECURITY</u>**:** Client platform devices, including State-owned assets, client devices used by remote workers and telecommuters, as well as third-party entities, connected to the budget unit’s internal network should be protected from sending or receiving hostile threats from unauthorized network traffic or software applications.

4.2.1. Client platform devices shall utilize virus-scanning software in accordance with *Statewide Standard P800-S860, Virus and Malicious Code Protection*.

4.2.2. Client platform devices externally connecting to budget unit internal networks shall encrypt all traffic in accordance with paragraph 4.6.

4.2.3. Individual firewalls deployed on client platform devices provide protection against network-borne threats by providing traditional firewall services blocking network traffic based on protocol, ports, and software applications, content filtering of packets, as well as controlling the behavior of software applications deployed and executed on the client platform device. Individual firewalls deployed on budget unit IT assets should be centrally administered and managed to ensure budget unit policy-based security is applied and updated.

4.3. <u>ACCESS TO INTERNETWORKING DEVICES AND SHARED PLATFORMS</u>**:** Internetworking devices (including routers, firewalls, switches, etc.) and shared platforms (including mainframes, servers, etc.) provide both access to and information about networks. They shall be controlled to prevent unauthorized access.

4.3.1. Access to Internetworking devices and shared platforms shall be restricted to authorized employees and contractors in accordance with *Statewide Standard P800-S885, Physical Security*, and *Statewide Standard P800-S875, Maintenance*.

4.3.2. Access to network management tools such as Simple Network Management Protocol (SNMP), Secure Socket Shell (SSH), and Remote Monitoring (RMON), etc., as well as telnet access, shall be controlled. SNMP shall be version 3 or higher to take advantage of improved security features.

4.3.3. Internetworking devices connected to the Internet shall have RFC 1918 and RFC 2827 implemented for inbound traffic.

4.3.4. If dial-in access is required to access and manage routers, RADIUS should be used.

4.3.5. Internetworking devices shall have unneeded services turned off, unused ports disabled, and logging capability turned on. Logs should be reviewed, on a frequency determined and documented by the budget unit, by budget unit authorized personnel and all incidents, violations, etc., reported and resolved.

4.3.6. Internetworking device passwords shall be immediately changed before or upon device installation and shall conform to requirements set forth in *Statewide Standard P800-S820, Authentication and Directory Services*, and budget unit specific password criteria.

4.3.7. Internetworking devices shall be configured to retain their current configuration, security settings, passwords, etc., during a reset or reboot process.

4.3.8. When disposing of internetworking devices that are no longer used by the budget unit, all configuration information shall be cleared in accordance with *Statewide Standard P800-S880, Media Sanitizing/Disposal*, to prevent disclosure of network configuration, keys, passwords, etc.

4.4. PATCH MANAGEMENT**:** Budget units shall develop and implement written procedures that identify roles and responsibilities for implementing patch management that include the following activities:

4.4.1. Designated budget unit employees or contractors shall proactively monitor and address software vulnerabilities of all internetworking devices in their network (routers, firewalls, switches, etc) by ensuring that applicable patches are acquired, tested, and installed in a timely manner. IT device manufacturers, security organizations, security vendors, and the Arizona Department of Administration (ADOA) Statewide Infrastructure Protection Center (SIPC) provide various tools and services to assist in identifying vulnerabilities and respective patches.

4.4.2. Where practical and feasible, budget units shall test patches in a test environment prior to installing the patch. Testing exposes detrimental impacts to internal/external enterprise-wide application software systems, community-of-interest application software systems, and other third-party application software systems.

4.4.3. Budget units shall query SIPC prior to installing patches in production to determine if other State budget units have experienced problems during testing or post-installation. Budget units shall report testing and production problems discovered with patches to SIPC.

4.4.4. Patches shall be installed (use of an automated tool is recommended) on all affected internetworking devices. Designated employees or contractors shall monitor the status of patches once they are deployed.

4.4.5. Patches make changes to the configuration of an internetworking device designed to protect and secure internetworking devices and attached IT devices and systems from attack, and shall be controlled and documented in accordance with *Statewide Standard P800-S815, Configuration Management*.

4.5. DEMILITARIZED ZONE**:** Services provided through the Internet (Web-enabled applications, FTP, Mail, DNS, VoIP, etc.) shall be deployed on a Demilitarized Zone (DMZ) or proxied from the DMZ.

4.5.1. All communication from servers on the DMZ to internal applications and services shall be controlled.

4.5.2. Remote or dial-in access to networks shall be authenticated at the firewall, or through services placed on the DMZ.

4.5.3. The DMZ is the appropriate location for web servers, external DNS servers, Virtual Private Networks (VPNs), and dial-in servers.

4.5.4. Budget-unit external DNS servers should neither be primary servers nor permit zone transfers to DNS servers outside of the budget unit.

4.5.5. All remote access users shall be considered external and therefore should be subjected to the firewall rule set. VPNs should terminate on the external segment or outside of the firewall.

4.6. EXTERNAL CONNECTION TO NETWORKS: External connections to networks shall be routed through secure gateways (as required above) and protected by at least one of the following encryption methods, as appropriate:

4.6.1. Transport Layer Security (TLS) or Secure Socket Layer (SSL) shall be employed between a web server and browser to authenticate the web server and, optionally, the user's browser. Implementations of TLS and SSL shall allow for client authentication support using the services provided by Certificate Authorities.

4.6.2. Wireless Transaction Layer Security (WTLS) with strong authentication and encryption shall be used between a web server and the browser of a wireless mobile device, such as a cellular telephone, PDA, etc., to provide sufficient levels of security during data transmission. WTLS currently supports X.509, X9.68 and WTLS certificates.

4.6.3. IP Security (IPSec) shall be used to extend the IP communications protocol, providing end-to-end confidentiality for data packets traveling over the Internet. The appropriate mode of IPSec shall be used commensurate with the level of security required for the data being transmitted: sender authentication and integrity without confidentiality or sender authentication and integrity with confidentiality.

4.6.4. VPNs shall be used to connect two networks or trading partners that must communicate over insecure networks, such as the public Internet, by establishing a secure link, typically between firewalls, using a version of the IPSec security protocol. VPNs are recommended for use in remote access.

4.6.5. Remote Authentication Dial-In User Service (RADIUS) which is a client/server protocol and software that enables network access servers to communicate with a central server to authenticate remote users and authorize their access to the requested system or service, and strong authentication shall be used for dial-up modem systems.

4.6.6. Dial-up desktop workstation modems should be disabled and removed. Use hardware and inventory scanning tools to verify the presence and configuration of dial utilities and modems. Budget units using dial-up modem systems shall establish modem use policies which include:

-
- A complete, current list of all authorized personnel having modem access privileges.
- Automatic disconnection after a specified period of inactivity. Inactivity parameters shall be determined by the budget unit.
- The recommended use of security tokens.
- Immediate termination of modem access privileges upon employment transfer, re-assignment, or termination.

4.6.7. Strong authentication, such as challenge/response devices, one-time passwords, tokens, Kerberos, and smart cards, shall be used once permission to connect has been granted.

4.6.8. External connections shall be removed promptly when no longer required. Key network components shall be disabled or removed to prevent inadvertent reconnection.

4.7. <u>INTER-NETWORK TRANSPORT SERVICES</u>**:** Generally and commercially available transport services, commonly referred to as carrier services, are defined in *Statewide Standard P710-S710, Network Infrastructure*. Based on budget unit business requirements, these services should be configured and implemented to allow for automatic re-routing of communications when critical nodes or links fail, or fall-back to alternate transport services, including the provision of duplicate or alternate secure gateways and external exchanges or switching centers.

4.8. WIRELESS NETWORK ACCESS**:** The 802.1x security standards having centralized user authentication in accordance with *Statewide Standard P800-S820, Authentication and Directory Services*, encryption technologies with automated key distribution, and VPN technologies shall be used as appropriate with standard wireless networks: IEEE 802.11x (Wireless Local Area Network (WLAN)), IEEE 802.15 (Wireless Personal Area Network (WPAN)), and IEEE 802.16 (Wireless Metropolitan Area Network (WMAN)).

4.8.1. WLAN security is being addressed in the transmission layer with the IEEE 802.11i draft standard and at the IP applications layer with standards- and policy-based authentication and access control.

- The Wired Equivalent Privacy (WEP) algorithm, which is part of the 802.11 standard, is susceptible to compromise; therefore, improved security methods should be considered.
- The Wireless Application Protocol (WAP) standard and Protected Extensible Authentication Protocol (PEAP) with the IEEE 802.1x Network Port Authentication standard provides interim, improved security until approval and widespread adoption of 802.11i.
- 802.11i also allows for automatically generated per user, per session keys through 802.1x. In addition, keys can be regenerated (re-keying) periodically to increase security.
- Vendor-specific, proprietary, security solutions may provide more enhanced interim security prior to approval and widespread adoption of 802.11i.

4.8.2. WLAN wireless access point device security:

- The service set identifier (SSID) shall be changed from the factory default setting.
- The broadcast SSID feature should be disabled, requiring wireless clients to scan for a specific access point.
- The default cryptographic key shall be changed from the factory default setting. Key management should change cryptographic keys often.
- Access point devices shall be managed via network management tools using SNMPv3 or higher. If network management is not performed by the budget unit, SNMP shall be disabled.
- Access point devices should be turned off during off-hours when not in use.

4.8.3. WLAN wireless client platforms connecting to budget unit networks using public access points and the Internet shall use VPN technologies and should use centrally managed individual firewall software solutions. Wireless client platforms utilizing VPN technologies to access internal networks and mission-critical software applications[1] improve security and decrease certain vulnerabilities inherent in unprotected wireless connectivity.

[1] Mission-critical software applications are those that address health, life, and safety issues; provide critical public services; or have been prescribed by legal mandates.

4.8.4. WPAN client devices used for network access, internal network-based Internet access, and application software access shall:

- Be required to adhere to the same range of security requirements as WLAN client devices defined in this Statewide standard.
- Require PIN entry or similar authentication in accordance with *Statewide Standard P800-S820, Authentication and Directory Services*, for all access.
- Require device-mutual authentication for all accesses.
- Invoke link encryption for all connections in the communication chain and encryption for all broadcast transmissions.
- Be set to the lowest necessary and sufficient power level so that transmissions remain localized.
- Require device passwords to prevent unauthorized use if lost or stolen.
- Use application-level encryption, authentication and VPN technologies.
- Be turned off during off-hours when not in use.

4.8.5. WMAN connectivity, commonly used to interconnect buildings, to internal networks that include transmissions to access internal networks and mission-critical software applications shall be encrypted and use VPN technologies.

4.8.6. *Statewide Standard P800-S850, Encryption Technologies*, describes minimum requirements for ensuring the authenticity, integrity, confidentiality, and reliability of digital information.

4.8.7. Passwords for wireless devices shall conform to requirements set forth in *Statewide Standard P800-S820, Authentication and Directory Services*, and budget unit specific password criteria.

4.8.8. Firewall technologies implemented at wireless application gateways and connection points between wireless and wire-based LANs additionally reduce unauthorized access to internal networks.

4.9. <u>INTRUSION DETECTION/PREVENTION</u>**:** Intrusion detection mechanisms or intrusion prevention tools should be incorporated into all servers connected to WANs and to all internetworking devices that serve as gateways between WAN network segments.

4.9.1. When used, intrusion detection systems shall be installed both external and internal to firewall technology protecting the network to monitor, block, and report unauthorized activity. Logs should be reviewed by budget unit authorized personnel and all incidents, violations, etc., reported and resolved.

4.9.2. Intrusion detection mechanisms for servers shall include the use of software and review procedures that scan for unauthorized changes to files, including system files.

4.9.3. Software and review procedures shall examine network traffic for known, suspicious attack signatures or activities and look for network traffic indicative of devices that have been misconfigured.

4.9.4. Violations of set parameters shall trigger appropriate notification to security administrators or budget unit staff, allowing a response to be undertaken.

4.9.5. Intrusion prevention tools combine user-defined security parameters with the ability to learn how software applications and operating systems should perform in their normal states to generate an appropriate set of security policies. Violations of these security policies produced through network penetration and changes in the normal state result in recognition of an attack with corresponding adjustments to stop it.

4.9.6. Application Vulnerability Description Language (AVDL) is a security interoperability standard being proposed as an OASIS standard. AVDL creates a uniform way of describing application security vulnerabilities using XML. The XML-based technology will allow communication between products that find, block, fix, and report application security holes.

4.9.7. Intrusion prevention technologies reduce the number of false alarms by focusing on real-time behavior rather than using signature-matching technology to identify a potential network attack. Intrusion prevention technologies can also prevent “zero-day” attacks, which exploit previously unknown weaknesses, because they respond to a change in the normal state of operation.

4.10. <u>VULNERABILITY SCANNING</u>: Network and host vulnerability scanners should be used to test for the vulnerabilities of internal systems and of network perimeter defenses, as well as adherence to security policy and standards. Vulnerability scanners should be components of the State’s comprehensive network security solutions. Such components allow security administrators to measure security, manage risk, and eliminate vulnerabilities, providing a more secure network environment. Scanners should have the ability to do the following:

4.10.1. Map the network or inventorying systems and services on the budget unit’s network,

4.10.2. Identify security holes by confirming vulnerabilities

4.10.3. Provide effective analysis if vulnerability data using browsing techniques, and enforcing valid security policies when used during security device installation and certification.

4.10.4. Provide comprehensive reports and charts for effective decision making and improved security, and

4.10.5. Define and enforce valid security policies when used during security device installation and certification.

4.11. <u>DESTRUCTION OF NETWORK DOCUMENTATION</u>: Hardcopy and electronic documentation of network device configurations, network diagrams, etc., shall be destroyed, as appropriate, when superseded, or no longer needed.

5. DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the GITA website at http://www.azgita.gov/policies_standards/ for definitions and abbreviations.

6. REFERENCES

6.1. A. R. S. § 41-621 et seq., "Purchase of Insurance; coverage; limitations, exclusions; definitions."
6.2. A. R. S. § 41-1335 ((A (6 & 7))),"State Agency Information."
6.3. A. R. S. § 41-1339 (A),"Depository of State Archives."
6.4. A. R. S. § 41-1461, "Definitions."
6.5. A. R. S. § 41-1463, "Discrimination; unlawful practices; definition."
6.6. A. R. S. § 41-1492 et seq., "Prohibition of Discrimination by Public Entities."
6.7. A. R. S. § 41-2501 et seq., "Arizona Procurement Codes, Applicability."
6.8. A. R. S. § 41-3501, "Definitions."
6.9. A. R. S. § 41-3504, "Powers and Duties of the Agency."
6.10. A. R. S. § 41-3521, "Information Technology Authorization Committee; members; terms; duties; compensation; definition."
6.11. A. R. S. § 44-7041, "Governmental Electronic Records."
6.12. Arizona Administrative Code, Title 2, Chapter 7, "Department of Administration Finance Division, Purchasing Office."
6.13. Arizona Administrative Code, Title 2, Chapter 10, "Department of Administration Risk Management Section."
6.14. Arizona Administrative Code, Title 2, Chapter 18, "Government Information Technology Agency."
6.15. Statewide Policy P100, Information Technology.
6.16. Statewide Policy P710, Network Architecture.
  6.16.1. Statewide Standard P710-S710, Network Infrastructure.
6.17. Statewide Policy P800, IT Security.
  6.17.1. Statewide Standard P800-S815, Configuration Management.
  6.17.2. Statewide Standard P800-S820, Authentication and Directory Services.
  6.17.3. Statewide Standard P800-S850, Encryption Technologies.
  6.17.4. Statewide Standard P800-S860, Virus and Malicious Code Protection.
  6.17.5. Statewide Standard P800-S875, Maintenance.
  6.17.6. Statewide Standard P800-S880, Media Sanitizing/Disposal.
  6.17.7. Statewide Standard P800-S885, IT Physical Security.
6.18. State of Arizona Target Security Architecture, http://www.azgita.gov/enterprise_architecture.

7. ATTACHMENTS

None.